AMENDMENTS TO THE CLAIMS

1. (currently amended) A method of operating a communication network, comprising:

autonomously monitoring communication traffic at a communication port for an anomalous traffic;

detecting an anomaly in communication traffic at a plurality of nodes in the communication network, wherein the anomaly is an attack other than a worm or virus;

independently applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

independently determining, at the respective ones of the plurality of nodes, a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to ~~the anomalous traffic stops~~ stop the anomalous traffic.

2. (Original) The method of claim 1, wherein independently determining the second blocking measure B comprises:

applying a logical combination of A and a second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and

enforcing the logical combination (A & !B), if the logical combination (A & !B) stops the anomalous traffic.

3. (currently amended) The method of claim 2, further comprising:

independently determining a third blocking measure C, at the respective ones of the plurality of nodes, such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & !B) stops the anomalous traffic.

4. (currently amended) The method of claim 2, wherein independently determining the second blocking measure B further comprises:

applying a logical combination (A & B) to the anomalous traffic if the logical

combination (A & !B) does not stop the anomalous traffic; and

enforcing the logical combination (A & B), if the logical combination (A & B) stops the anomalous traffic.

5. (currently amended) The method of claim 4, further comprising:

independently determining a third blocking measure C_x at the respective ones of the plurality of nodes, such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) stops the anomalous traffic.

6. (currently amended) The method of claim 4, further comprising:

determining a third blocking measure C_x at the respective ones of the plurality of nodes, such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) does not stop the anomalous traffic.

7. (Original) The method of claim 1, wherein detecting an anomaly in the communication traffic comprises:

comparing the communication traffic to at least one anomaly factor; and

detecting the anomaly in the communication traffic at the plurality of nodes in the communication network if the at least one anomaly factor is present in the communication traffic.

8. (Original) The method of claim 1, further comprising:

assigning a severity to the detected anomaly; and

wherein independently applying the first blocking measure A to the anomalous traffic comprises independently applying the first blocking measure A to the anomalous traffic at each of the plurality of nodes in the communication network that stops or reduces the flow of the anomalous traffic based on the severity of the detected anomaly.

9. (Original) The method of claim 1, further comprising:

intentionally inserting the anomaly in the communication traffic; and

associating the first blocking measure A and the second blocking measure B with the anomaly.

10. (currently amended) A method of operating a communication network, comprising:

detecting an anomaly in communication traffic at a plurality of nodes in the communication network;

synchronously applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

synchronously determining, at the respective ones of the plurality of nodes, a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to ~~the anomalous traffic stops~~ stop the anomalous traffic.

11. (currently amended) A system for operating a communication network, comprising:

a processor;

program means executing on the processor including:

means for autonomously monitoring communication traffic at a communication port for an anomalous traffic;

means for detecting an anomaly in communication traffic at a plurality of nodes in the communication network, wherein the anomaly is an attack other than a worm or virus;

means for independently applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

means for independently determining, at the respective ones of the plurality of nodes a, second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to ~~the anomalous traffic stops~~ stop the anomalous traffic.

12. (currently amended) The system of claim 11, wherein the means for independently determining the second blocking measure B comprises:

means for applying a logical combination of A and a second blocking measure B given

by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and

means for enforcing the logical combination (A & !B), if the logical combination (A & !B) stops the anomalous traffic.

13. (currently amended) The system of claim 12, further comprising:

means for independently determining, at the respective ones of the plurality of nodes, a third blocking measure C such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & !B) stops the anomalous traffic.

14. (Original) The system of claim 12, wherein the means for independently determining the second blocking measure B further comprises:

means for applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and

means for enforcing the logical combination (A & B), if the logical combination (A & B) stops the anomalous traffic.

15. (currently amended) The system of claim 14, further comprising:

means for independently determining, at the respective ones of the plurality of nodes, a third blocking measure C such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) stops the anomalous traffic.

16. (currently amended) The system of claim 14, further comprising:

means for determining, at the respective ones of the plurality of nodes, a third blocking measure C such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) does not stop the anomalous traffic.

17. (currently amended) The system of claim 11, wherein the means for detecting an anomaly in the communication traffic comprises:

means for comparing the communication traffic to at least one anomaly factor; and

means for detecting the anomaly in the communication traffic at the plurality of nodes in the communication network, if the at least one anomaly factor is present in the communication traffic.

18. (Original) The system of claim 11, further comprising:

means for assigning a severity to the detected anomaly; and

wherein the means for independently applying the first blocking measure A to the anomalous traffic comprises means for independently applying the first blocking measure A to the anomalous traffic at each of the plurality of nodes in the communication network that stops or reduces the flow of the anomalous traffic based on the severity of the detected anomaly.

19. (Original) The system of claim 11, further comprising:

means for intentionally inserting the anomaly in the communication traffic; and

means for associating the first blocking measure A and the second blocking measure B with the anomaly.

20. (currently amended) A system for operating a communication network, comprising:

means for detecting an anomaly in communication traffic at a plurality of nodes in the communication network;

means for synchronously applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

means for synchronously determining a second blocking measure B at the respective ones of the plurality of nodes such that application of a logical combination of the first blocking measure A and the second blocking measure B to ~~the anomalous traffic stops~~ stop the anomalous traffic.

21. (currently amended) A computer program product for operating a communication network,

comprising:

a tangible computer ~~readable~~ storage medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code configured to autonomously monitor communication traffic at a communication port for an anomalous traffic;

computer readable program code configured to detect an anomaly in communication traffic at a plurality of nodes in the communication network, wherein the anomaly is an attack other than a worm or virus;

computer readable program code configured to independently apply, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

computer readable program code configured to independently determine at the respective ones of the plurality of nodes a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to ~~the anomalous traffic stops~~ stop the anomalous traffic.

22. (Original) The computer program product of claim 21, wherein the computer readable program code configured to independently determine the second blocking measure B comprises:

computer readable program code configured to apply a logical combination of A and a second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and

computer readable program code configured to enforce the logical combination (A & !B) if the logical combination (A & !B) stops the anomalous traffic.

23. (currently amended) The computer program product of claim 22, further comprising:

computer readable program code configured to independently determine, at the respective ones of the plurality of nodes, a third blocking measure C such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & !B) stops the anomalous traffic.

24. (currently amended) The computer program product of claim 22, wherein the computer readable program code configured to independently determine the second blocking measure B further comprises:

computer readable program code configured to apply a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and

computer readable program code configured to enforce the logical combination (A & B), if the logical combination (A & B) stops the anomalous traffic.

25. (currently amended) The computer program product of claim 24, further comprising:

computer readable program code configured to independently determine, at the respective ones of the plurality of nodes, a third blocking measure C such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) stops the anomalous traffic.

26. (currently amended) The computer program product of claim 24, further comprising:

computer readable program code configured to determine, at the respective ones of the plurality of nodes, a third blocking measure C such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) does not stop the anomalous traffic.

27. (currently amended) The computer program product of claim 21, wherein the computer readable program code configured to detect an anomaly in the communication traffic comprises:

computer readable program code configured to compare the communication traffic to at least one anomaly factor; and

computer readable program code configured to detect the anomaly in the communication traffic at the plurality of nodes in the communication network, if the at least one anomaly factor is present in the communication traffic.

28. (Original) The computer program product of claim 21, further comprising:

computer readable program code configured to assign a severity to the detected anomaly; and

wherein the computer readable program code configured to independently apply the first blocking measure A to the anomalous traffic comprises computer readable program code configured to independently apply the first blocking measure A to the anomalous traffic at each of the plurality of nodes in the communication network that stops or reduces the flow of the anomalous traffic based on the severity of the detected anomaly.

29. (Original) The computer program product of claim 21, further comprising:

computer readable program code configured to intentionally insert the anomaly in the communication traffic; and

computer readable program code configured to associate the first blocking measure A and the second blocking measure B with the anomaly.

30. (currently amended) A computer program product for operating a communication network, comprising:

a tangible computer ~~readable~~ storage medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code configured to detect an anomaly in communication traffic at a plurality of nodes in the communication network;

computer readable program code configured to synchronously apply, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

computer readable program code configured to synchronously determine at the respective ones of the plurality of nodes a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to ~~the anomalous traffic stops~~ stop the anomalous traffic.